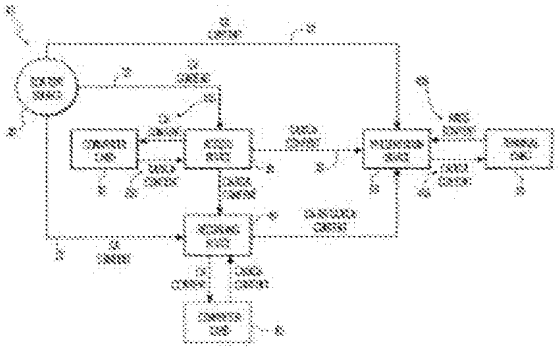
METHOD AND SYSTEM FOR HANDLING TWO CA SYSTEMS IN A SAME RECEIVER

Publication number: JP2003511917 (T)
Publication date: 2003-03-25
Inventor(s):
Applicant(s):
Classification:
- international: ***H04L9/32; H04N5/00; H04N7/16; H04N7/173;*** **H04L9/32; H04N5/00; H04N7/16; H04N7/173;** (IPC1-7): H04L9/32; H04N7/173
- European: H04N5/00M4; H04N7/16E
Application number: JP20010529207T 20001006
Priority number(s): US19990157968P 19991006; WO2000US27685 20001006

Also published as:
WO0126372 (A1)
MXPA02003524 (A)
ES2225240 (T3)
EP1226717 (A1)
EP1226717 (B1)
more >>

Abstract not available for JP 2003511917 (T)
Abstract of corresponding document: **WO 0126372 (A1)**

A method for enabling a security device to enable an audio/video processing system to permit access to a service, by correctly identifying the service and entitlement message packet. The audio/video transmission systems use multiple conditional access identifications.



(19)日本国特許庁（ＪＰ）　(12)**公表特許公報（Ａ）**　(11)特許出願公表番号
特表2003－511917
（P2003－511917A）
(43)公表日　平成15年３月25日(2003.3.25)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｎ　7/173	６３０	Ｈ０４Ｎ　7/173	６３０	５Ｃ０６４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｚ	５Ｊ１０４

審査請求　未請求　予備審査請求　有　（全 36 頁）

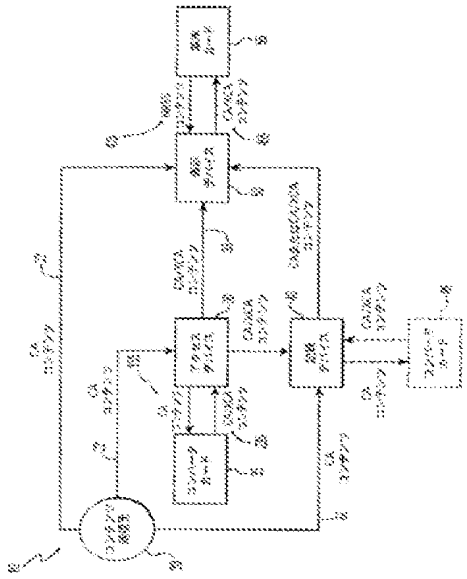
(21)出願番号　特願2001－529207(P2001－529207)
(86)(22)出願日　平成12年10月６日(2000.10.6)
(85)翻訳文提出日　平成14年４月８日(2002.4.8)
(86)国際出願番号　ＰＣＴ／ＵＳ００／２７６８５
(87)国際公開番号　ＷＯ０１／０２６３７２
(87)国際公開日　平成13年４月12日(2001.4.12)
(31)優先権主張番号　６０／１５７，９６８
(32)優先日　平成11年10月６日(1999.10.6)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　トムソン　ライセンシング　ソシエテ　アノニム
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ　Ｓ．Ａ．
フランス国，　エフ－92100　ブローニュ　ビヤンクール，　ケ　アルフォンス　ルガロ，　46番地
(72)発明者　アーメット　ムルジット　エスキシオグル
アメリカ合衆国　46250　インディアナ州　インディアナポリス　ナンバー125　レイクショア　トレイル　8235
(74)代理人　弁理士　谷　義一　（外２名）

最終頁に続く

(54)【発明の名称】　同じ受信機において２つのＣＡシステムを扱うための方法およびシステム

(57)【要約】
サービスおよび資格メッセージパケットを正確に識別することによって、オーディオ／ビデオ処理システムがサービスへのアクセスを許可できるようにすることをセキュリティデバイスに可能にするための方法。オーディオ／ビデオ伝送システムは、複数の条件付きアクセス識別を使用する。



【特許請求の範囲】

【請求項１】　オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、所定の規定に従って前記抽出された対のうちの１つを自動的に識別すること

を含むことを特徴とする方法。

【請求項２】　所定の規定が、前記セキュリティデバイスに前記対が送信される順番によって異なることを特徴とする請求項１に記載の方法。

【請求項３】　前記受信した対のそれぞれが、関連付けられた条件付きアクセス（ＣＡ）システムか、拡張条件付きアクセス（ＸＣＡ）システムのどちらかであることを特徴とする請求項１に記載の方法。

【請求項４】　オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、

サービスおよび資格制御メッセージパケット識別子の対が１つだけ抽出された場合、前記抽出された対を識別し、

サービスおよび資格制御メッセージパケット識別子の複数の対が抽出された場合、所定の規定に従って前記抽出された対のうちの少なくとも１対を自動的に識別すること

を含むことを特徴とする方法。

【請求項５】　所定の規定が、前記対が抽出された順番によって異なることを特徴とする請求項４に記載の方法。

【請求項６】　前記受信した対のそれぞれが、条件付きアクセス資格制御メッセージ識別子か、ローカル資格制御メッセージ識別子のどちらかを含むことを特徴とする請求項５に記載の方法。

【請求項７】　前記受信した対のそれぞれが、サービス識別子をさらに含むことを特徴とする請求項６に記載の方法。

【請求項８】　前記所定の規定が、受信されるべき対の第１の対をサービス識別子およびローカル資格制御メッセージ識別子を含むと定義することを特徴とする請求項６に記載の方法。

【請求項９】　前記データの少なくとも一部が、複数の条件付きアクセスシステムのうちの１つを用いてセキュリティ保護されることを特徴とする請求項４に記載の方法。

【請求項１０】　前記条件付きアクセスシステムのうちの少なくとも１つが、前記プログラムの放送業者に関連付けられており、少なくとも第２の条件付きアクセスシステムがアクセスデバイスに関連付けられており、前記表示デバイスと通信可能であることを特徴とする請求項９に記載の方法。

【請求項１１】　前記表示デバイスがデジタルテレビジョンであり、前記アクセスデバイスが第２のセキュリティデバイスと組み合わされたセットトップボックスであることを特徴とする請求項１０に記載の方法。

【請求項１２】　セキュリティデバイスが、インターフェース保護関連情報と条件付きアクセス関連情報とをオーディオ／ビデオ処理デバイスに伝達すること、および

オーディオ／ビデオ処理デバイスが、前記伝達された条件付きアクセス情報と記憶されている条件付きアクセス情報とを用いてプログラムマップテーブルを分解することを含み、

前記プログラムマップテーブルがパケット識別子を対応するサービス情報に関連付けることを特徴とする請求項４に記載の方法。

【請求項１３】　前記プログラムを示すデータをデスクランブルするのに適した資格制御メッセージデータをどのパケットが含んでいるかを識別するために、前記セキュリティデバイスが、パケット識別子を使用することを特徴とする請求項１２に記載の方法。

【請求項１４】　前記資格制御メッセージの少なくともいくつかが、少なくとも、識別およびＬＥＣＭ用フィールドと、条件付きアクセス識別用フィールドとを含むローカル資格制御メッセージであり、前記正当な処理が、前記識別およびＬＥＣＭ用フィールドと前記条件付きアクセス識別用フィールドのうちの少な

くとも１つに含まれる情報を用いて前記データの適切な鍵にアクセスすることによって前記サービスをデスクランブルすることを含むことを特徴とする請求項１３に記載の方法。

【請求項１５】　前記データの少なくとも１つの部分が少なくとも１つのプログラムを示すことを特徴とする請求項９に記載の方法。

【請求項１６】　前記データがデジタル伝送システムを介して伝達されることを特徴とする請求項４に記載の方法。

【発明の詳細な説明】

【０００１】

（発明の分野）

本発明は、一般に、デジタルオーディオ／ビデオ伝送システムに関し、より詳細には、デジタルオーディオ／ビデオ伝送システム内の受信機に複数の条件付きアクセス識別を使用することを可能にする方法およびシステムに関する。

【０００２】

（発明の背景）

ＩＳＯ／ＩＥＣ　１３８１８－１は、オーディオおよびビデオの１つまたは複数の基本ストリームならびに他のデータの、記憶および伝送に適した単一または複数のストリームへのコーディングを規定する国際規格である。プログラムストリーム（ＰＳ）コーディングとトランスポートストリーム（ＴＳ）コーディングの２つの形式のコーディングが推奨される。コーディングのプロセスでは、パケット化エレメンタリストリーム（ＰＥＳ）を獲得するために、まずオーディオビジュアル（Ａ／Ｖ）ストリームが圧縮されてパケット化される。ＰＳは、１つまたは複数のストリームのＰＥＳパケットを共通の時間基準で結合して単一ストリームにする。ＴＳは、１つまたは複数のプログラムを１つまたは複数の個別の時間基準で結合して単一ストリームにする。ＰＳパケットは様々な長さであってよいが、ＴＳパケットは１８８バイトの長さである。各ＴＳパケットは、パケット内に含まれるデータのタイプを識別するパケットＩＤ（ＰＩＤ）を伴う４バイトのヘッダーを有する。ＰＥＳパケットに加え、ＴＳは、多重分離するためのプログラム仕様情報（ＰＳＩ）テーブルと現在のプログラムから構成される。プログラムマップテーブル（ＰＭＴ）は、プログラム番号とそれらを含んでいるエレメントとの間でマッピングを実現するテーブルである。これは、各プログラムに関連付けられたＰＩＤのリストを含む。

【０００３】

アドバンストテレビジョンシステム委員会（ＡＴＳＣ）は、地上波放送のためのその条件付きアクセス（ＣＡ）システムのためにサイマルクリプトアーキテクチャを既に採用している。このアーキテクチャでは、各サービスは、複数の異な

る独自開発システムに対して、資格管理メッセージ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍｅｎｔ Ｍｅｓｓａｇｅ：ＥＭＭ）と資格制御メッセージ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ：ＥＣＭ）と共に送信される。この方法で、異なるＣＡシステムを使用するデコーダは、様々な資格メッセージを信号で伝えるための共通フレームワークを用いてサービスを復号することができる。各サービスは、オーディオパケットとビデオパケットで構成されている。どのデコーダも、それが必要とするパケットを選定し、ストリーム内の他のパケットを無視する。

【０００４】

サイマルクリプトベースのＣＡシステムでは、デジタルテレビジョン（ＤＴＶ）等のデジタルオーディオ／ビデオ処理システムは、ＰＭＴを分解し、ＣＡモジュールから獲得したＣＡシステム識別（ＩＤ）を用いてサービスおよびＥＣＭ ＰＩＤを抽出する。通常、各ＣＡモジュールは、１つのＣＡシステムだけをサポートし、したがって１つのＣＡシステムＩＤだけを有する。Ａ／ＶパケットのＰＩＤと制御ワード（ＣＷ）を伝えるＥＣＭのＰＩＤとが、正規の購入資格を有するプログラムをデスクランブルするＣＡモジュールに送信される。

【０００５】

（発明の概要）

本発明は、オーディオ／ビデオ処理デバイスがＰＭＴを分解するために２つのＣＡシステムＩＤを使用することを可能にし、ＣＡモジュールが特定ＣＡシステムに属するＥＣＭ ＰＩＤを正確に識別することを可能にする。本発明は、Ａ／Ｖ処理デバイス例えばＤＴＶが、セキュリティデバイスに、サービスおよび資格制御メッセージ用パケットを正確に識別することによってプログラムにアクセスすることを可能にする方法を含む。このセキュリティデバイスはＡ／Ｖ処理デバイスに関連付けられており、このＡ／Ｖ処理デバイスは、サービスに関連付けられたデータのためにデジタル送信システムに関連付けられている。この方法は、データからサービスおよび資格メッセージ制御パケット識別子の対を少なくとも１つ抽出すること、サービスおよび資格制御メッセージパケット識別子の対が１つだけ抽出された場合、その抽出された対を識別すること、および、サービスお

よび資格制御メッセージパケット識別子の複数の対が抽出された場合、所定の規則に従ってその抽出された対のうちの１つを自動的に選択することを含む。

【０００６】

（発明の詳細な説明）

図１は、放送源から、すなわちコンテンツ送信元２０を介してコンテンツを受信し、ＸＣＡおよびＮＲＳＳコピー防止システム（後述）による保護を提供するネットワーク１０を示す。コンテンツ送信元２０は、例えばテープ、ＤＶＤ、ケーブル、衛星放送、地上波放送のいづれによっても、経済的価格のあるＣＡコンテンツ２２を提供することができる。コンテンツ２２は、通常、保護されており、私設ＣＡネットワークの加入者に供給されるＡ／Ｖコンテンツを含んでいる。購入した加入者、またはコンテンツ２２を受信する資格を有する加入者には、コンテンツ２２をデスクランブルするための必須の鍵が供給される。図１の実施形態によれば、コンテンツ送信元２０は、このＣＡコンテンツ２２をアクセスデバイス３０、記録デバイス４０または表示デバイス５０に提供することができる。

【０００７】

アクセスデバイス３０は、セットトップボックスの形態をとることができる。セットトップボックス３０は、ＸＣＡ／ＮＲＳＳコンバータカード３５と共に動作して、ＣＡコンテンツ２２からＸＣＡ保護されたコンテンツを作成するが、それはＣＡ／ＸＣＡコンテンツ３３の一部になる。記録デバイス４０は、デジタルＶＨＳ（ＤＶＨＳ）またはＤＶＤレコーダの形態をとることができる。記録デバイスは、コンバータカード３５に類似したコンバータカード４５に提供されても提供されなくてもよい。表示デバイス５０は、ＤＶＤの形態をとり、ＣＡ／ＸＣＡ保護されたコンテンツをデスクランブルするためにＸＣＡ／ＮＲＳＳ端末カード５５と共に動作することができる。

【０００８】

拡張条件付きアクセス（Ｅｘｔｅｎｄｅｄ　Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ：ＸＣＡ）は、コンテンツの配信および販売用の既成および新規のモデルをサポートしながら、伝送および記憶中にＭＰＥＧ２符号化デジタルＡ／Ｖコンテンツを保護するためのシステムである。ＸＣＡは、「再生」および「記録」と

いう基本的な制御を表示制御にマッピングすることによってこのタスクを達成する。ＸＣＡシステムにおいて、経済的価格のあるコンテンツは常にスクランブルされている。すなわち、これらのコンテンツは配信者の制御および責任下にあるか、または消費者の家庭、例えばローカル、ネットワークの範囲内にあるものである。ＸＣＡはスクランブルされたコンテンツの記録を可能にするが、但しそれは合法的なコピーだけをデスクランブルし、表示することができるということである。非合法なコンテンツは、デスクランブルされないので、表示することはできない。非合法なコンテンツとは、例えば原作でないものや著作権所有者の承認を受けていないもののことである。

【０００９】

ＸＣＡは３段階の資格を提供する。無制限に自由に配信されるコンテンツは、「コピー自由」コンテンツである。このコンテンツの例としては、広告が流され、提供を受けている放送テレビジョン、インフォマーシャル、または類似の素材を挙げることができる。「１回コピー済み（ｃｏｐｙ－ｏｎｃｅ）」またはローカル表示プログラミングコンテンツは、単一の家庭またはローカルネットワーク内で作成され、何回でも表示することができる。しかしながら、このようなコピーは他のローカルネットワークに転送することができない。このタイプのコンテンツの例としては、スポーツイベントまたは割増金サービスを挙げることができる。最後に「コピー不可」または即時表示プログラミングコンテンツは、リアルタイム表示だけを可能にし、すなわち記録されたコピーは表示不可能である。このタイプのコンテンツの例としては、従量料金制プログラミングまたは他の高額コンテンツを挙げることができる。

【００１０】

ＸＣＡアーキテクチャに特徴的な特性は、条件付きアクセスとローカルプロテクションの概念である。ローカルプロテクションまたはセキュリティは、アクセスデバイス、例えば３０が、スクランブルされたプログラム、例えばＣＡコンテンツ２２を受信した後における、ホームネットワークの範囲内におけるコンテンツの保護である。これは、表示デバイス、例えば５０が、何に対してアクセス権を有しており、したがって、保護されているどのコンテンツを変換し、表示する

ことができるかを規定している。取り外し可能なセキュリティデバイス、例えばコンバータカードおよび端末カード３５、４５、５５は、セキュリティ関連の機能を実施する。経済的価値のあるコンテンツはＣＡサービスを使用して配信される。例えばデジタル衛星システムは、そのシステムの加入者に対する大量配信用ビデオコンテンツおよび鍵をスクランブルする。一部の加入者はそのコンテンツの購入を決定することができるが、その場合、その加入者にはそのコンテンツをデスクランブルして表示するために必須の鍵が供給される。コンテンツを購入しないことを選択した加入者には、これらの鍵へのアクセス権は提供されない。ＸＣＡでは、デスクランブルするための鍵は、一意のローカル公開鍵によって保護される新しいＥＣＭに再バンドルされる。ローカルＥＣＭ（ＬＥＭＣ）を使用してコンテンツを受信する表示デバイスは、したがって特定のＣＡシステムによって保護されるコンテンツだけを処理するのではなく、同様にＸＣＡによって保護されるコンテンツを処理することも必要となる。

【００１１】

次に図２を参照すると、システム１０における使用に適した汎用ＸＣＡ家庭用電化製品（ＣＥ）デバイス６０が示されている。特定のタイプのデバイス６０は特有の機能を有している。例えばＸＣＡアクセスデバイス３０はＣＡ／ＸＣＡ３３に対するＸＣＡ保護されたコンテンツを作成し、ＸＣＡ表示デバイス５０はＸＣＡ保護されたコンテンツをデスクランブルし、ＸＣＡ記録デバイス４０は、コンバータカード４５が提供されていない限り、ＸＣＡ保護されたコンテンツを記憶し、再生はするが、これを作成したりデスクランブルすることはできない。一般に、汎用デバイス６０には、切替ユニット（ｓｗｉｔｃｈｉｎｇ　ｕｎｉｔ）６２、入力ユニット６１、および更新可能なまたは組込み型のセキュリティデバイス６６、例えばコンバータカード３５または４５、または端末カード５５が含まれる。そのデバイスのタイプによって、デバイス６０には、表示ユニット６４、記憶ユニット６８、アナログ出力６５、圧縮解除されたデジタル出力６７または圧縮されたデジタル出力６９も含まれる場合がある。

【００１２】

デジタル入力ユニット６１は、一般に、例えば復調器等の、デジタル信号を獲

得するために必要な回路およびソフトウェアを含む。圧縮されたデジタル出力６９は、例えば変調器等の、ＭＰＥＧ２デジタル信号を発行するための回路およびソフトウェアを使用する。セキュリティデバイス６６は、ＣＡ機能とＸＣＡ機能とを操作してコンテンツのタイプを変換することができる。これは、変換されたコンテンツをデジタル形式で出力するモデルの唯一の素子である。前述の通り、セキュリティデバイス６６は、コンバータカード３５または４５、または端末カード５５の形式をとることができる。コンバータカード３５および４５は、（ｉ）ＣＡ資格を検査すること、（ｉｉ）制御ワード（ＣＷ）回復、（ｉｉｉ）コンテンツのデスクランブル等の機能をサポートする。これは、三重データ暗号化規格（ＴＤＥＳ）鍵を生成し、そのコンテンツを再スクランブルし、その公開鍵を使用してＬＥＣＭを暗号化する。端末カード５５は、ＸＣＡ資格を検査すること等の機能をサポートする。これは、ＬＥＣＭのＣＷを用いてコンテンツをデスクランブルし、次いでＸＣＡ　ＮＲＳＳインターフェース保護システムの要件に従ってそのコンテンツを再スクランブルする。例示的コンバータカード３５と端末カード５５のブロック図を、それぞれ図３および図４に示す。記憶ユニット６８は、不揮発性メモリにコンテンツを記憶し、そこからコンテンツを読み出す。記憶ユニット６８は、コンバータカード４５が提供されていない限りコンテンツのタイプを変換せず、その場合、記憶ユニット６８はアクセスデバイスとしても動作する。ハードディスクは典型的な内部記憶ユニットである。デジタル揮発性ディスク（ＤＶＤ）プレーヤおよび、ＤＶＨＳ等のデジタルビデオテープレコーダは、典型的な取り外し可能記憶装置付きＣＥデバイスである。表示ユニット６４は、ＭＰＥＧ２コンテンツを復号し、それをユーザにアナログ形式または圧縮解除されたデジタル形式で提示する。表示ユニットは、ＮＲＳＳデスクランブラー６４′を用いてＮＲＳＳストリームをデスクランブルすることができ、ＭＰＥＧデコーダ６４″を用いてデジタルストリームを復号することができ、デジタルアナログコンバータ（ＤＡＣ）６４‴を用いてデジタルアナログ変換を実施することができる。最終結果は、音声またはアナログ電子信号等の物理信号である場合がある。ハイファイ増幅器のＴＶディスプレイおよびアナログ出力は典型的な例である。切替ユニット６２は、デバイス６０内でコンテンツを経路指定する。

その機能は経路指定のみに限定され、コンテンツのタイプは変更しない。

【００１３】

ＸＣＡシステムは、ＸＣＡ端末カード５５を表示デバイス５０に接続するＮＲＳＳインターフェースを保護するように設計されている。コンテンツがＣＡ／ＸＣＡコンテンツなので、ＮＲＳＳインターフェース保護はアクセスデバイス３０では必要とされない。

【００１４】

ＸＣＡ保護されたＮＲＳＳインターフェースを設定する手順では、表示ホストデバイス５０を認証すること、特定の表示デバイス５０／端末カード５５の対に対して一意の共用秘密鍵を設定すること、コンテンツ保護用共用鍵を作成すること、データ暗号化規格（ＤＥＳ）および共用鍵によってホスト５０に戻るコンテンツをスクランブルすること。

【００１５】

ローカル資格制御メッセージ（ＬＥＣＭ）は、表１のシンタックスによって長さが可変であることができる１つまたは複数のセクションに含めることができる。セクションの始めは、パケットペイロードのポインタフィールドで示すことができる。

【００１６】

【表１】

表１

シンタックス		ビット数	ニーモニック
Local_Entitlement)Control_Message{			
	Table_id	8	0×80 または 0×81
	Section_syntax_indicator	1	'1'
	Private_indicator	1	'1'
	Zero	2	'00'
	Private_section_length	12	Uimsbf
	Table_id_extension(){		
	Reserved	6	'000000'
	LECM_type	2	'10'
	Protocol_version	8	Uimsbf
	}		
	Reserved	2	'11'
	Version_number	5	'00000'
	Current_next_indicator	1	'1'
	Section_number	8	0×00
	Last_section_number	8	0×00
	XCA_indentifier	256	Uimsbf
	Local_source_id	64	Uimsbf
	Reserved	5	Uimsbf
	Copy_protect_enable	1	Uimsbf
	XCA_view_flag	2	Uimsbf
	Time_code	32	Uimsbf
	Source_sequence_number	32	Uimsbf
	XCA_descriptor	424	Uimsbf
	Padding_bytes	508	Uimsbf
	Integrity_check	32	Uimsbf
	CRC_32	32	Rpchof

【００１７】

ここで、

Ｔａｂｌｅ＿ｉｄ　この８ビットフィールドは、このセクションが属している資格制御メッセージを識別する。０×８０または０×８１のどちらかにセットされる。ＬＥＣＭセクションにおいて少なくとも１ビットの変更がある場合、このｔａｂｌｅ＿ｉｄは切り替わる。

【００１８】

Ｓｅｃｔｉｏｎ＿ｓｙｎｔａｘ＿ｉｎｄｉｃａｔｏｒ　この１ビットのフィールドは「１」にセットされる。これは、そのセクションが、セクション長さフィールドを超えて汎用セクション構文に続くことを示している。

【００１９】

Ｐｒｉｖａｔｅ＿ｉｎｄｉｃａｔｏｒ　この１ビットのフィールドは「１」にセットされる。

【００２０】

Ｐｒｉｖａｔｅ＿ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈ　この１２ビットのフィールドは、ｐｒｉｖａｔｅ＿ｓｅｃｔｉｏｎ＿ｌｅｎｇｔｈフィールド直後から続けて始まり、ＣＲＣ＿３２を含めて、このセクション内の残りのバイト数を明記する。

【００２１】

ＬＥＣＭ＿ｔｙｐｅ　この２ビットのフィールドは、ＬＥＣＭによって伝えられる情報のタイプを示す。「１０」は、これが制御ワードを伝えていることを意味している。

【００２２】

Ｐｒｏｔｏｃｏｌ＿ｖｅｒｓｉｏｎ　８ビットの符号のない整数フィールドであって、その機能は、現行プロトコルにおいて定義されているパラメータと異なって構造化し得るパラメータを、将来、この表が伝えることを可能にするものである。現在はプロトコルが１つだけ定義されている。Ｐｒｏｔｏｃｏｌ＿ｖｅｒｓｉｏｎ＝０ｘ００の場合、プログラム全体に対して単一の制御ワードの対が使用され、同様に、プログラム全体に対してアクセス基準が規定される（すなわち、ストリームレベルの保護は許可されない）。この場合、その事象のすべてのストリームは同じ制御ワードによってスクランブルされ、同じアクセス基準を使用する。Ｐｒｏｔｏｃｏｌ＿ｖｅｒｓｉｏｎ＝＞０．０１の場合、０×００よりも大きなｐｒｏｔｏｃｏｌ＿ｖｅｒｓｉｏｎの値は、そのプロトコルの将来のバージョンが導入された際にそのバージョンに合わせて設計されたデコーダによって処理されることだけが可能である。

【００２３】

Ｖｅｒｓｉｏｎ＿ｎｕｍｂｅｒ　この５ビットのフィールドは予約されており、「００００００」の値を有する。将来の実施態様は、必要に応じてこのフィールドを使用することができる。

【００２４】

Ｃｕｒｒｅｎｔ＿ｎｅｘｔ＿ｉｎｄｉｃａｔｏｒ　この１ビットのインジケータはＬＥＣＭのために常に「１」にセットされており、送信されるＬＥＣＭは常に現行で適用可能である。

【００２５】

Ｓｅｃｔｉｏｎ＿　ｎｕｍｂｅｒ　この８ビットのフィールドは、いくつかのプライベートセクションを含んでいる。プライベートテーブル内の第１のセクションのセクション番号は０×００になる。このセクション番号は、このプライベートテーブルに属する付属セクションごとに１つずつ増分される。

【００２６】

Ｌａｓｔ＿ｓｅｃｔｉｏｎ＿ｎｕｍｂｅｒ　この８ビットのフィールドは、このセクションをその一部として含むプライベートテーブルの最後のセクション番号を示している。

【００２７】

ＸＣＡ＿ｉｄｅｎｔｉｆｉｅｒ　この２５６ビットのフィールドは一意のＸＣＡ識別子を含んでいる。この識別子は、「著作権：（Ｃ）１９９９　ＴＭＭ」というＡＳＣＩＩ値を有する。引用符は含まれない。各ＡＳＣＩＩ文字には１バイトの記憶が割り当てられている。このフィールドでは文字は左寄せされる。未割当てのフィールド値は０×００にセットされる。

【００２８】

Ｌｏｃａｌ＿ｓｏｕｒｃｅ＿ｉｄ　この６４ビットのフィールドは、このＬＥＣＭを生成したセキュリティデバイスのＸＣＡデバイスＩＤを含んでいる。

【００２９】

Ｃｏｐｙ＿ｐｒｏｔｅｃｔ＿ｅｎａｂｌｅ　この１ビットのフィールドは、表示デバイスから出力されるプログラムマテリアルの１つまたは複数のストリー

ムのためのコンテンツ保護機構があることを示す。このフラッグの目的は、ユーザに対して故障表示を検出するための手段を提供することであり、コピー防止を強制するために使用されるものではない。少なくとも１つのストリームに対する保護が使用可能である場合、このフィールドの値は「１」にセットされる。

【００３０】

ＸＣＡ＿ｖｉｅｗ＿ｆｌａｇ　この２ビットのフィールドの値は、ＸＣＡ保護に変換する前にプログラムコンテンツの保護を管理する管理権限によって判定される。この値は、ＸＣＡ＿ｄｅｓｃｒｉｐｔｏｒにおけるＸＣＡ＿ｖｉｅｗ＿ｆｌａｇの値と照合される。不一致の場合、ＸＣＡ表示デバイスのセキュリティプロセッサ内で表示権を行使するために、保護されるＸＣＡ＿ｖｉｅｗ＿ｆｌａｇが使用される。意味体系は以下の通りである。

【００３１】

ＸＣＡ＿ｖｉｅｗ＿ｆｌａｇ＝′００′：ＸＣＡコンテンツは制限されない。いつでも、どこでも表示してよい。ＸＣＡ＿ｖｉｅｗ＿ｆｌａｇ＝′０１′：ＸＣＡは予約されている。ＸＣＡ＿ｖｉｅｗ＿ｆｌａｇ＝′１０′：ＸＣＡコンテンツはローカルネットワーク内ではいつでも表示してよいという制限を受ける。ＸＣＡ＿ｖｉｅｗ＿ｆｌａｇ＝′１１′：ＸＣＡコンテンツはローカルネットワーク内で「今」だけ表示してよいという制限を受ける。

【００３２】

Ｔｉｍｅ＿ｃｏｄｅ　タイムソースが周知でありセキュリティ保護されている場合、このフィールドは、１９８０年ＵＴＣ１月６日午前１２時から発生している秒数を含んでいる（ｍｏｄ２[※]）。タイムソースが周知でもなくセキュリティ保護もされていない場合、このフィールドはすべて０に符号化される。

【００３３】

Ｓｏｕｒｃｅ＿ｓｅｑｕｅｎｃｅ＿ｎｕｍｂｅｒ　この３２ビットのフィールドは、ＬＥＣＭを作成したコンバータモジュールの暗号期間カウンタを含んでいる。

【００３４】

Ｐａｄｄｉｎｇ＿ｂｙｔｅｓ　ＬＥＣＭのセキュリティ保護された部分の合

計の長さ（１２８－６５）を１２８バイトにするために必要とされるバイト数である。このｐａｄｄｉｎｇ＿ｂｙｔｅはランダムに選択される。

【００３５】

Ｉｎｔｅｇｒｉｔｙｃｈｅｃｋ　この３２ビット数のフィールドは、暗号解除されたペイロードのコンテンツが有効であることを確認する値を含んでいる。これは、暗号化プロセスと暗号解除プロセスとが適切に実施されることを保証するために使用される。

【００３６】

ＣＲＣ－３２　この３２ビットのフィールドは、ＬＥＣＭセクション全体を処理した後でＩＳＯ／ＩＥＣ　１３８１８－１「ＭＥＰＧ２Ｓｙｓｔｅｍｓ」付録Ａで定義されているデコーダのレジスタからのゼロ出力を保証するためのＣＲＣ値を含んでいる。この値は、データが暗号化された後で計算される。

【００３７】

各コンバータカード３５は、ＣＡ保護されたコンテンツからＸＣＡ保護されたコンテンツへの変換をサポートし、３２ビットの暗号期間カウンタを有する。暗号期間は、ストリームまたはプログラムが１つの特定の鍵によってスクランブルされる期間と定義される。新しい暗号期間ごとに、すなわち、制御ワードが変更する度に、コンバータモジュールはその暗号期間カウンタを１つ増分する。例えばプログラムが異なる暗号期間を有する３つのストリームを含む場合、このカウンタは各ストリームの各暗号期間の開始時点で増分される。外部からのアクセスに対して保護されているので、このカウンタがリセットされたり減らされたりすることは有り得ない。暗号期間の初期値は０である。

【００３８】

コンバータカード３５は、そのコンテンツへのアクセスが合法であると判定すると、ＬＥＣＭを作成するために次の情報を使用する。すなわち、奇数と偶数のＣＷ、コピー制御情報（ＣＣＩ）、および、例えば「表示自由」、「ローカル表示のみ」、「現時点での表示のみ」の３つの実現可能な状況のうちの１つであるようなコピー防止（ＣＰ）状況である。

【００３９】

ＣＡ保護されたコンテンツからＸＣＡ保護されたコンテンツへの変換は次のプロセスを含む。すなわち、コンバータカード３５がそのＸＣＡ＿ＩＤをＬｏｃａｌ＿ｓｏｕｒｃｅ＿ｉｄに割り当てる。コンバータカード３５は、コンテンツが「現時点での表示のみ」のタイプである場合はｃｏｐｙ＿ｐｒｏｔｅｃｔ＿ｅｎａｂｌｅを１にセットし、そうでない場はｃｏｐｙ＿ｐｒｏｔｅｃｔ＿ｅｎａｂｌｅは０にセットされる。コンバータカード３５は暗号期間カウンタの現行値をｓｏｕｒｃｅ＿ｓｅｑｕｅｎｃｅ＿ｎｕｎｂｅｒに割り当てる。また、コンバータカードは、ＬＥＣＭのセキュリティ保護された部分で計算されたハッシュ値をｉｎｔｅｇｒｉｔｙ＿ｃｈｅｃｋに割り当てる、というプロセスである。

【００４０】

ハッシュ方法は、本発明の一態様によれば以下の通りである。

【００４１】

【数１】

$$C[0] = M[0] \oplus M[4] \oplus \ldots \oplus M[4 \times (n/4)]$$
$$C[1] = M[1] \oplus M[5] \oplus \ldots \oplus M[4 \times ((n-1)/4) + 1]$$
$$C[2] = M[2] \oplus M[6] \oplus \ldots \oplus M[4 \times ((n-2)/4) + 2]$$
$$C[3] = M[3] \oplus M[7] \oplus \ldots \oplus M[4 \times ((n-3)/4) + 3]$$

【００４２】

上式で、Ｍ［ｉ］は、暗号化すべきメッセージのｉ番目のバイトを表しており、シーケンスの第１のバイトは指標０を有しており、Ｃ［ｉ］はｉｎｔｅｇｒｉｔｙ＿ｃｈａｃｋフィールドのｉ番目のバイトを表しており、フィールドの第１のバイトは指標０を有する。

【００４３】

ＬＥＣＭのセキュリティ保護された部分はＲＳＡ－１０２４を使用して暗号化される。暗号化鍵は、コンテンツが「表示自由」のタイプの場合は自由表示公開鍵であるＫｐｕｂ＿ｆｒｅｅであり、そうでない場合、これはコンバータカードの公開鍵であるＫｐｕｂ＿ｉである。最後に、コンバータカードは、ＬＥＣＭのセキュリティ保護された部分を暗号化した後でＣＲＣ＿３２を計算する。

【００４４】

再び図３を参照すると、例示的コンバータカード３５のブロック図が示されている。コンバータカード３５は、ＣＡシステム１００と、ＸＣＡシステム２００とを含む。ＣＡシステム１００は、一般に、リンク３７を介してホストデバイスと通信するＩＳＯ―７８１６リンクデバイス１１０、例えばアクセスデバイス３０と、ＣＡ操作可能ソフトウェア（ＳＷ）１２０と、ＥＣＭおよびＥＭＭ抽出器（ｅｘｔｒａｃｔｏｒ）１３０、１４０と、三重日付暗号化規格（ＴＤＥＳ）デバイス１５０とを含む。ＴＤＥＳデバイス１５０、およびＥＣＭおよびＥＭＭ抽出器１３０、１４０には、ホストからＣＡコンテンツを受信するための入力１５５が設けられ、供給されている。ＴＤＥＳデバイス１５０は出力１６０をさらに含む。ＸＣＡシステム２００は、一般に、ＸＣＡ操作可能ソフトウェア２２０とＥＣＭ置換モジュール２３０とを含む。ＥＭＣ置換モジュール２３０は、出力１６０を介してＴＤＥＳ変換モジュール１５０と通信することができる。ＥＣＭ置換モジュール２３０には、ホストにＸＣＡコンテンツを戻すための出力２３５がさらに提供されている。

【００４５】

端末カード５５は、ＸＣＡ保護されたコンテンツからＮＲＳＳコンテンツへの変換をサポートする。この目的のために、端末カード５５は、それ自体に連結されているコンバータカード３５（ｉ）ごとにその記録を保持する。この記録は以下のフィールドを含んでいる。すなわち、コンバータカード３５（ｉ）のＸＣＡ＿ＩＤ、コンバータカード３５（ｉ）の秘密鍵Ｋｐｒｉｖ＿ｉ、およびコンバータカード３５（ｉ）から受信したｓｏｕｒｃｅ＿ｓｅｑｕｅｎｃｅ＿ｎｕｍｂｅｒＳＳＮｉの最新の値である。ＸＣＡ保護されたコンテンツからＮＲＳＳコンテンツへの変換には、ＣＲＣ＿３２の値がＬＥＣＭから計算された値と一致しない場合、端末カード５５がその変換を取り消すことを含む。ＸＣＡ＿ｖｉｅｗ＿ｆｌａｇによって定義されるコンテンツの状況が「表示自由」のタイプに相当する場合、暗号解除鍵は自由表示秘密鍵Ｋｐｒｉｖ＿ｆｒｅｅである。端末カード５５は、ＲＳＡ－１０２４を使用してＬＥＣＭのセキュリティ保護された部分の暗号解除を行う。暗号化されていないｌｏｃａｌ＿ｓｏｕｒｃｅ＿ｉｄから、端末

カード５５は発行しているコンバータカード３５を識別する。端末カード５５が対応する秘密鍵をまだ有していない場合、すなわち、端末カード５５が、その第１のフィールドがｌｏｃａｌ＿ｓｏｕｃｅ＿ｉｄの値に等しい記録を有していない場合、端末カード５５はその変換を停止し、秘密鍵の要求を開始する。そうでない場合、端末カード５５は、ｌｏｃａｌ＿ｓｏｕｃｅ＿ｉｄで識別されるコンバータカード３５に関連付けられた秘密鍵を使用して、ＲＳＡ－１０２４でＬＥＣＭのセキュリティ保護された部分を暗号解除する。未暗号化部分のＸＣＡ＿ｖｉｅｗ＿ｆｌａｇの値がＸＣＡ記述子のＸＣＡ＿ｖｉｅｗ＿ｆｌａｇの値と一致しない場合、端末カード５５はその変換を取り消す。コンテンツが「現時点での表示のみ」タイプに相当する場合、端末カード５５は、２つの検査によって再生がないことを保証する。セキュリティ保護されたタイムソースがホストに対して使用可能でない場合、第１の検査は省略される。第１の検査において、端末カード５５は、ｔｉｍｅ＿ｃｏｄｅを、ＮＲＳＳコマンドを用いて表示デバイス５０から受信したホストタイムと照合する。その差が所定の量、例えば５分よりも多い場合、端末カード５５はＳＳＮｉをｓｏｕｒｃｅ＿ｓｅｑｕｅｎｃｅ＿ｎｕｍｂｅｒと照合する。そうでない場合、端末カード５５はその変換を取り消す。第２の検査では、ＳＳＮｉがｓｏｕｃｅ＿ｓｅｑｕｅｎｃｅ＿ｎｕｍｂｅｒよりも少ない場合、端末カード５５は対応するＳＳＮｉを更新し、ＬＥＣＭのＣＷを用いてコンテンツをデスクランブルする。そうでない場合、端末カード５５はその変換を取り消す。コンテンツが「現時点での表示のみ」タイプに相当しない場合、端末カード５５はＬＥＣＭのＣＷを用いてコンテンツをデスクランブルする。端末カード５５は、ＣＣＩフィールドのコンテンツをＮＲＳＳ保護の目的でＮＲＳＳモジュール３００に渡す。最後に、端末カード５５は、ＮＲＳＳモジュール３００にそれぞれの新しい暗号期間の発生を伝達する。

【００４６】

別の変換では、ＸＣＡ保護されたコンテンツはクリアコンテンツに変換される。この変換は、ＸＣＡ保護されたコンテンツをＮＲＳＳコンテンツに変換することに類似しているが、これらの顕著な違いは、例えばクリアコンテンツはデバイス６０の切替ユニット６２に直接的に渡され、ＣＣＩはホストプロセッサに直接

的に渡されるということである。

【００４７】

再び図４を参照すると、例示的端末カード５０のブロック図が示されている。一般に、端末カード５０は、ＣＡシステム４００とＸＣＡシステム３００とを含む。ＣＡシステム４００は、一般に、ホストデバイスと通信可能なＩＳＯ―７８１６リンクデバイス４１０、例えばリンク５７を介する表示デバイス５０と、ＣＡ操作可能ソフトウェア（ＳＷ）４２０と、ＥＣＭおよびＥＭＭ抽出器４３０、４４０と、三重日付暗号化規格（ＴＤＥＳ）デスクランブルデバイス４５０とを含む。ホストからＣＡ／ＸＣＡコンテンツを受信するための入力４５５がＴＤＥＳデバイス４５０、ＥＣＭおよびＥＭＭ抽出器４３０、４４０に設けられ、供給されている。ＴＤＥＳデバイス４５０は、出力４６０をさらに含んでいる。ＸＣＡシステム３００は、一般に、ＸＣＡ操作可能ソフトウェア３２０、ＮＲＳＳコピー防止操作可能ソフトウェア（ＳＷ）３４０、およびＮＲＳＳコピー防止（ＣＰ）モジュール３５０とを含む。ＮＲＳＳコピー防止（ＣＰ）モジュール３５０は、出力４６０を介してＴＤＥＳデスクランブルモジュール４５０と通信可能である。ＮＲＳＳコピー防止（ＣＰ）モジュール３５０には、ＮＲＳＳコンテンツをホストに戻すための出力４３５もさらに設けられている。

【００４８】

端末カード５５は、それ自体のタスクを完了するために、ホストデバイス５０とデータを交換する。この通信は、例えばＮＲＳＳ　ＥＩＡ－６７９Ｂ準拠コマンドを用いて実行することができる。該当するＮＲＳＳ規格によれば、どの動作を実行する必要があるかを決定するためにホストは定期的にカードの状況を監視する。

【００４９】

ナショナルリニューアブルセキュリティスタンダード（ＮＲＳＳ：Ｎａｔｉｏｎａｌ　Ｒｅｎｅｗａｂｌｅ　Ｓｅｃｕｒｉｔｙ　Ｓｔａｎｄａｒｄ）は、継続可能なセキュリティを、ＤＴＶ受信機およびデジタルＶＣＲ等のデジタル家庭電化（ＣＥ）デバイスで使用するための手段を提供する。したがってこのセキュリティ機能は、ナビゲーショナルデバイス（ｎａｖｉｇａｔｉｏｎａｌ　ｄｅｖｉ

ｃｅ）からは分離されている。端末カード５５のようなＮＲＳＳセキュリティデバイスは、表示デバイス５０のようなそのホストデバイスから保護されたコンテンツを受信すると、そのコンテンツをデスクランブルし、それをホストデバイスに返送する。コンテンツはセキュリティデバイスを離れる前はクリアな状態なので、インターフェース全体を通して保護される必要がある。ＮＲＳＳ規格は、また、暗号ベースのコピー防止システムに対するフレームワークを定義する。

【００５０】

ＮＲＳＳ規格によれば、ホストと端末カードは、１つまたは複数のＮＲＳＳコピー防止システムに対するサポートを有するように製造することができる。これらのシステムは、一意のコピー防止（ＣＰ）システムＩＤによって識別される。どのシステムが実施されるかを判定するために、端末カード５５とそのホストデバイス５０との間でネゴシエーションを使用することができる。端末カード５５の初期化の一部として、ホスト５０は、それがサポートするＮＲＳＳコピー防止システムに関して端末カード５５に報告する。ＸＣＡ　ＮＲＳＳコピー防止システムがこのセットに含まれている場合、端末カード５５は、ＣＡシステムＩＤをも含むその構成と共にＣＰシステムＩＤを返送する。この構成を検討して、ホスト５０は、ＸＣＡと特定のＣＡシステムの両方が端末カード５５によってサポートされていることを認識し、その後、ＸＣＡシステムＩＤとＣＡシステムＩＤの両方を用いてＰＭＴを分解する。新しいプログラムごとに、カード５５はホストからサービスとＥＣＭ　ＰＩＤを獲得する。本発明の一態様によれば、ＸＣＡ　ＣＡシステムＩＤは、それがデータの機密部分でないかのようにＸＣＡコピー防止システムをサポートするホストデバイスに記憶されており、セキュリティ保護された記憶装置を必要としない。

【００５１】

構造によって、端末カード５５は、放送事業者のヘッドエンドおよびホームネットワークにおける再生デバイスを含めて、様々な送信元から入来するＣＡおよびＸＣＡストリームの両方を処理する。受信したコンテンツに応じて、ホスト、例えば表示デバイス５０は端末カード５５に｛サービスＰＩＤ、ＥＣＭ　ＰＩＤ｝の１つまたは複数の対を返送することができる。ここで、次の３つの可能性が

ある。すなわち（１）１対だけが送信される、すなわち、ＬＥＣＭ　ＰＩＤを含んでいる｛サービスＰＩＤ、ＥＣＭ　ＰＩＤ｝である。（２）１対だけが送信される、すなわち、ＣＡ　ＥＭＣ　ＰＩＤを含んでいる｛サービスＰＩＤ＞、ＥＣＭ　ＰＩＤ｝である。または（３）２対が送信される。すなわち、ＬＥＣＭを含んでいる１対と、ＣＡ　ＥＣＭ　ＰＩＤを含んでいるもう１対である。したがって、ＣＡ　ＥＣＭとＬＥＣＭとを区別する必要がある。２つの例示的ケースを提供する。

【００５２】

ケース（ａ）：２つの対が提供される場合。第１の対｛サービスＰＩＤ、ＥＣＭ　ＰＩＤ｝が、規定により、ＰＩＤのうちの所定の１つ、例えばＬＥＣＭ　ＰＩＤまたはＣＡ　ＥＣＭ　ＰＩＤと定義される。

【００５３】

ケース（ｂ）：１対だけが提供される場合。端末カードが、表１に関して議論したように、ＬＥＣＭをそれらのシンタックスを検査することによって検出する。本発明の別の態様によれば、この目的のために使用することができる２つのフィールドはＬＥＣＭ＿ｔｙｐｅとＸＣＡ＿ｉｄｅｎｔｉｆｉｅｒである。前者は転送パケットが伝えるものを示し、後者はＸＣＡ　ＬＥＣＭに対する一意の識別子を提供する。

【００５４】

例えば、（１）ビデオＰＩＤ：１００と、（２）オーディオＰＩＤ：１０１のサービスＰＩＤを有するＰＩＤを想定する。これら２つの基本ストリームは同一鍵によって保護される。デスクランブルする鍵は、２つのＣＡシステムによって保護されるＥＣＭで伝えられる（２つのＣＡシステムより多くのＣＡシステムがあってもよい）。すなわち、（１）ＣＡシステム＃１　ＥＣＭ　ＰＩＤ：１８０および（２）ＣＡシステム＃２　ＥＣＭ　ＰＩＤ：１８１である。ＣＡシステム＃１用のＥＣＭはＰＩＤ１８２を有するＬＥＣＭに変換され、置換される。次にホストデバイスは表２によって特徴づけられるように、カードに２つの対（サービスＰＩＤ、ＥＣＭ　ＰＩＤ）を送信する。

【００５５】

【表２】

表２

サービスＰＩＤ	ECMPID
100	182
101	182
100	181
101	181

【００５６】

複数対のうちの第１の対が規定によってＬＥＣＭ　ＰＩＣにセットされた場合、ＰＩＤ１８２はＬＥＣＭに対してＰＩＤであると識別される。

【図面の簡単な説明】

【図１】

放送源からコンテンツを受信し、ＸＣＡおよびＮＲＳＳコピー防止システムを使用してコピー防止を提供するように構成されているネットワークを示す図である。

【図２】

図１のシステム内で使用されているＸＣＡデバイスのブロック図である。

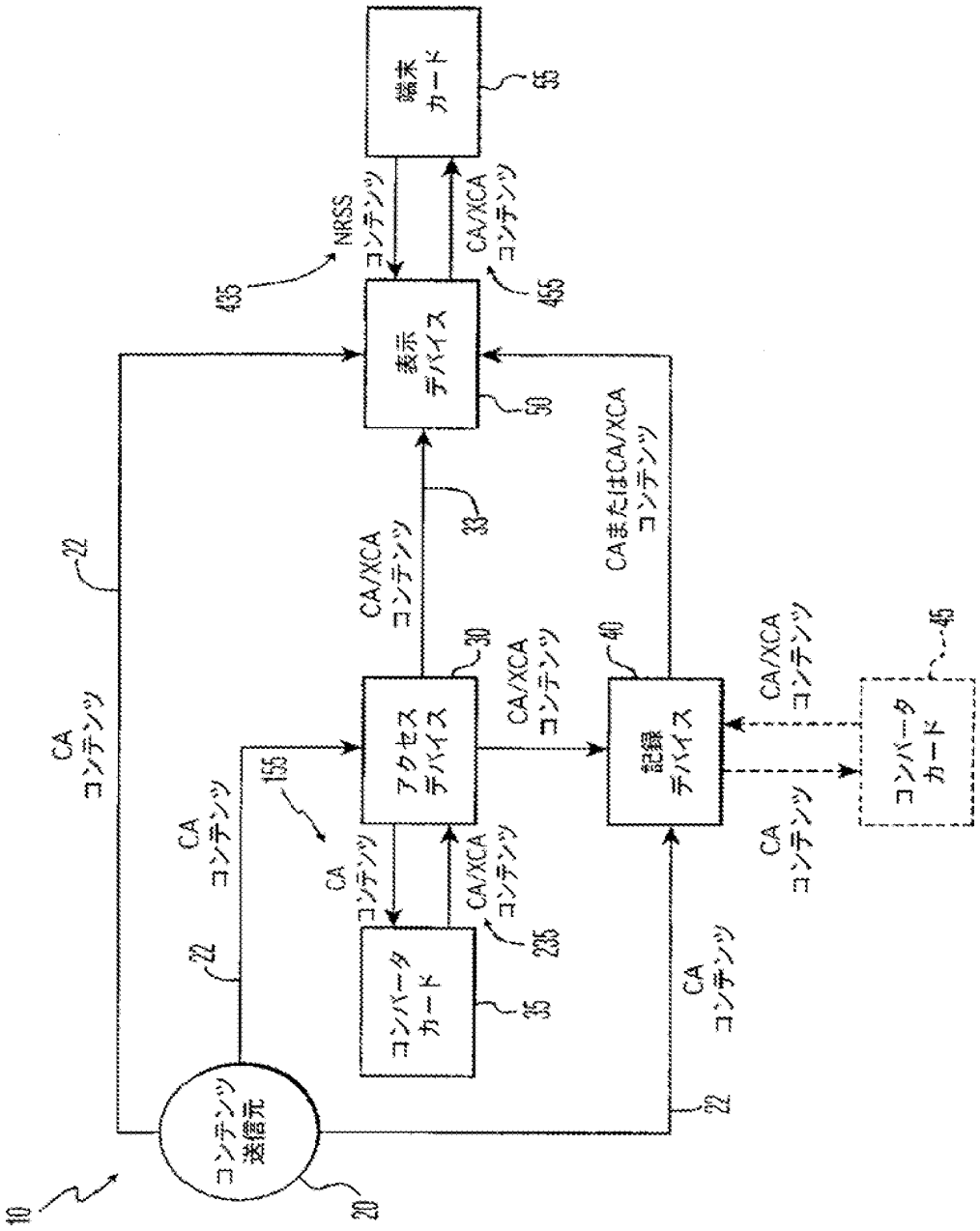
【図３】

本発明の一態様で利用されるコンバータカードのブロック図である。

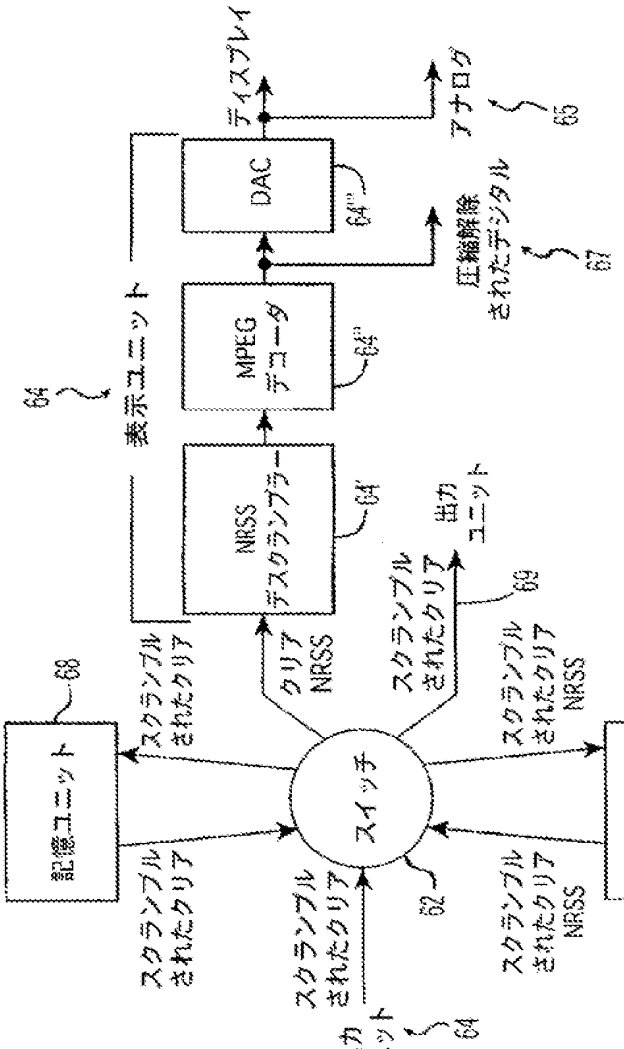
【図４】

本発明の一態様で利用される端末カードのブロック図である。

【図１】


端末カード
65
NRSSコンテンツ
435
CA/XCAコンテンツ
455
表示デバイス
50
33
CA/XCAコンテンツ
CAまたはCA/XCAコンテンツ
22
CAコンテンツ
155
アクセスデバイス
30
CA/XCAコンテンツ
記録デバイス
40
CA/XCAコンテンツ
コンバータカード
45
CAコンテンツ
CAコンテンツ
CA/XCAコンテンツ
235
コンバータカード
35
CAコンテンツ
22
コンテンツ送信元
20
10

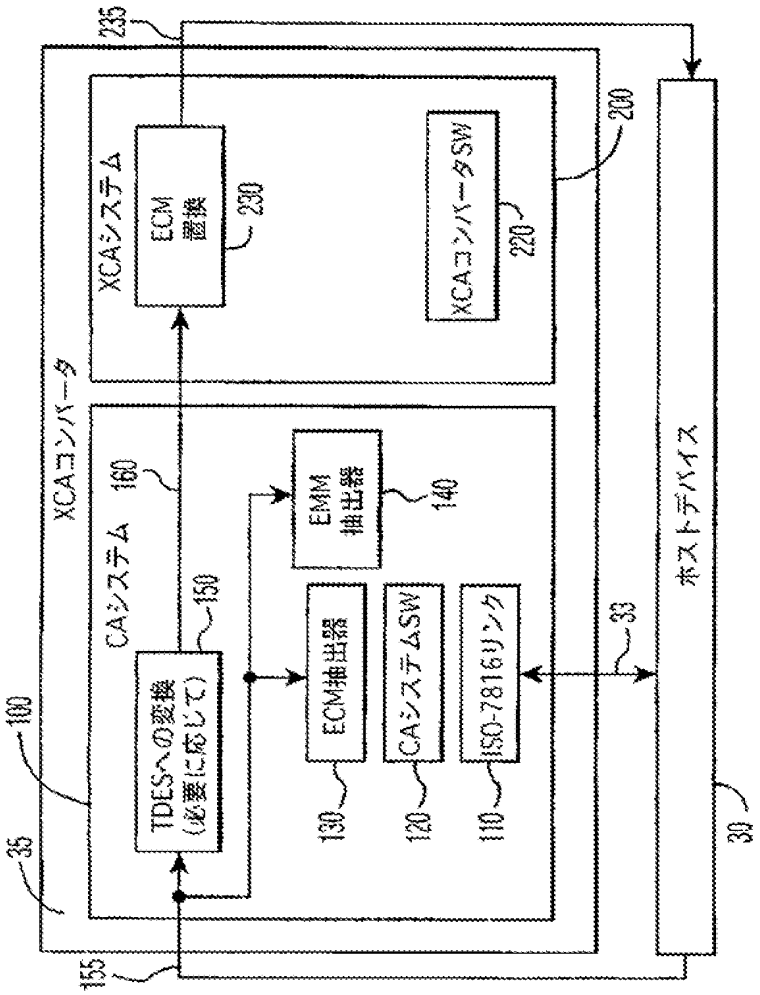
【図２】



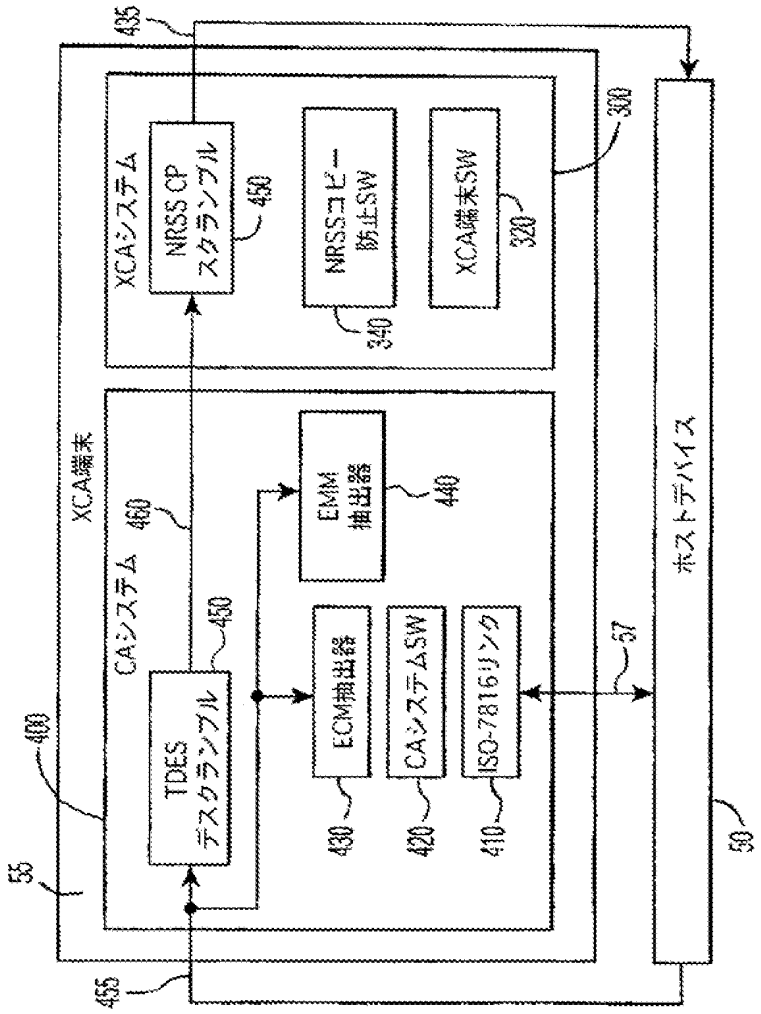
コンテンツのタイプ

スクランブルされたもの：CAおよびXCAコンテンツ。クリアなもの：未スクランブルのMPEG転送ストリーム。
NRSS：単一DESスクランブルされた転送ストリーム。このコンテンツは、1つまたは複数のデスクランブル
する鍵が使用不可能の場合、スクランブルされたコンテンツと判別不可能である。

【図３】


235
XCAコンバータ
XCAシステム
ECM
置換
230
XCAコンバータSW
220
200
CAシステム
160
EMM
抽出器
140
150
TDESへの変換
(必要に応じて)
ECM抽出器
CAシステムSW
ISO-7816リンク
130
120
110
100
35
155
33
ホストデバイス
30

【図４】


435
XCAシステム
NRSS CP
スクランブル
450
NRSSコピー
防止SW
340
XCA端末SW
320
300
XCA端末
460
CAシステム
450
EMM
抽出器
440
TDES
デスクランブル
ECM抽出器
CAシステムSW
ISO-7816リンク
430
420
410
400
55
57
ホストデバイス
50
455

【手続補正書】特許協力条約第３４条補正の翻訳文提出書

【提出日】平成１３年１０月２４日（２００１．１０．２４）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項１】　オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、所定の規定に従って前記抽出された対のうちの１つを自動的に識別することを含み、

前記受信した複数の対のそれぞれが、条件付きアクセス資格制御メッセージ識別子（ＣＡ　ＥＣＭ）またはローカル資格制御メッセージ識別子（ＬＥＣＭ）のどちらかを含むことを特徴とする方法。

【請求項２】　所定の規定が、前記セキュリティデバイスに前記対が送信される順番によって異なることを特徴とする請求項１に記載の方法。

【請求項３】　前記受信した対のそれぞれが、関連付けられた条件付きアクセス（ＣＡ）システムか、拡張条件付きアクセス（ＸＣＡ）システムのどちらかであることを特徴とする請求項１に記載の方法。

【請求項４】　オーディオ／ビデオ処理デバイスが、セキュリティデバイスがサービスにアクセスすることを可能にするための方法であって、

前記サービスに関連付けられたデータから、サービスおよび資格制御メッセージパケット識別子の対を抽出し、

サービスおよび資格制御メッセージパケット識別子の対が１つだけ抽出された場合、前記抽出された対を識別し、

サービスおよび資格制御メッセージパケット識別子の１以上の対が抽出された場合、所定の規定に従って前記抽出された対の少なくとも１つを自動的に識別す

ること

を含み、

前記受信した複数の対のそれぞれが、条件付きアクセス資格制御メッセージ識別子（ＣＡ　ＥＣＭ）またはローカル資格制御メッセージ識別子（ＬＥＣＭ）のどちらかを含む

ことを特徴とする方法。

【請求項５】　所定の規定が、前記対が抽出された順番によって異なることを特徴とする請求項４に記載の方法。

【請求項６】　前記受信した対のそれぞれが、サービス識別子をさらに含むことを特徴とする請求項４に記載の方法。

【請求項７】　前記所定の規定が、受信されるべき対の第１の対をサービス識別子およびローカル資格制御メッセージ識別子を含むと定義することを特徴とする請求項４に記載の方法。

【請求項８】　前記データの少なくとも一部が、複数の条件付きアクセスシステムのうちの１つを用いてセキュリティ保護されることを特徴とする請求項４に記載の方法。

【請求項９】　前記条件付きアクセスシステムのうちの少なくとも１つが、前記プログラムの放送業者に関連付けられており、少なくとも第２の条件付きアクセスシステムがアクセスデバイスに関連付けられており、前記表示デバイスと通信可能であることを特徴とする請求項８に記載の方法。

【請求項１０】　前記表示デバイスがデジタルテレビジョンであり、前記アクセスデバイスが第２のセキュリティデバイスと組み合わされたセットトップボックスであることを特徴とする請求項９に記載の方法。

【請求項１１】　セキュリティデバイスが、インターフェース保護関連情報と条件付きアクセス関連情報とをオーディオ／ビデオ処理デバイスに伝達すること、および

オーディオ／ビデオ処理デバイスが、前記伝達された条件付きアクセス情報と記憶されている条件付きアクセス情報とを用いてプログラムマップテーブルを分解することを含み、

前記プログラムマップテーブルがパケット識別子を対応するサービス情報に関連付けることを特徴とする請求項４に記載の方法。

【請求項１２】　前記プログラムを示すデータをスクランブル解除するのに適した資格制御メッセージデータをどのパケットが含んでいるかを識別するように、前記セキュリティデバイスが、パケット識別子を使用することを特徴とする請求項１１に記載の方法。

【請求項１３】　前記資格制御メッセージの少なくともいくつかが、少なくとも、識別およびＬＥＣＭ用フィールドと、条件付きアクセス識別用フィールドとを含むローカル資格制御メッセージであり、前記正当な処理が、前記識別およびＬＥＣＭ用フィールドと前記条件付きアクセス識別用フィールドのうちの少なくとも１つに含まれる情報を用いて前記データの適切な鍵にアクセスすることによって前記サービスをスクランブル解除することを含むことを特徴とする請求項１２に記載の方法。

【請求項１４】　前記データの少なくとも１つの部分が少なくとも１つのプログラムを示すことを特徴とする請求項８に記載の方法。

【請求項１５】　前記データがデジタル伝送システムを介して伝達されることを特徴とする請求項４に記載の方法。

【請求項１６】　放送業者資格制御メッセージからローカル資格制御メッセージを識別するための方法であって、

サービスおよび資格制御メッセージパケット識別子の対を、サービスに関連付けられたデータから抽出するステップと、

サービスおよび資格制御メッセージパケット識別子の対が１つだけ抽出された場合、前記抽出された対がローカル資格制御メッセージまたは放送資格制御メッセージのどちらかであることを確認するステップと、

サービスおよび資格制御メッセージパケット識別子の１以上の対が抽出された場合、前記抽出された対の少なくとも１つがローカル資格制御メッセージであることを自動的に確認するステップと

を含むことを特徴とする方法。

【請求項１７】　放送資格制御メッセージからローカル資格制御メッセージ

を識別するための方法であって、

サービスに関連付けられたデータからサービスおよび資格制御メッセージパケット識別子の対を抽出するステップと、

サービスおよび資格制御メッセージパケット識別子の対が１つだけ抽出された場合、前記抽出された対がローカル資格制御メッセージまたは放送資格制御メッセージのどちらかであることを確認するステップと、

サービスおよび資格制御メッセージパケット識別子の１以上の対が抽出された場合、前記抽出された対の少なくとも１つが放送資格制御メッセージであることを自動的に確認するステップと

を含むことを特徴とする方法。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０００４

【補正方法】変更

【補正の内容】

【０００４】

サイマルクリプトベースのＣＡシステムでは、デジタルテレビジョン（ＤＴＶ）等のデジタルオーディオ／ビデオ処理システムは、ＰＭＴを分解し、ＣＡモジュールから獲得したＣＡシステム識別（ＩＤ）を用いてサービスおよびＥＣＭＰＩＤを抽出する。通常、各ＣＡモジュールは、１つのＣＡシステムだけをサポートし、したがって１つのＣＡシステムＩＤだけを有する。Ａ／ＶパケットのＰＩＤと制御ワード（ＣＷ）を伝えるＥＣＭのＰＩＤとが、正規の購入資格を有するプログラムをスクランブル解除するＣＡモジュールに送信される。

Ｗａｓｉｌｅｗｓｋｉによる米国特許第５，４２０，８６６号は、サイマルクリプトシステムに酷似した複数の異なるデコーダに対して条件付きアクセス情報を提供するための方法を記載している。Ｗａｓｉｌｅｗｓｋｉは、異なるＣＡプロバイダを識別するためにＣＡシステム識別パラメータＣＡ＿Ｓｙｓｔｅｍ＿ＩＤ、したがって異なるデコーダを使用することを述べている（列１２、行１２－１６参照のこと）。

また、Ｄａｎｉｅｌ Ｋｒａｍｅｒによる「Ｗｕｎｄｅｒｋｉｓｔｅ ｄｅｓ ｄｉｇｉｔａｌｅｎ Ｆｅｒｎｓｅｈｅｎｓ」という名称の記事は、サイマルクリプト技術について記述している（Ｋｒａｍｅｒ Ｄ：「Ｗｕｎｄｅｒｋｉｓｔｅ ｄｅｓ ｄｉｇｉｔａｌｅｎ Ｆｅｒｎｓｅｈｅｎｓ」Ｂｕｌｌ、ＳＥＶ／ＶＳＥ、ＣＨ、Ｓｃｈｗｅｉｚｅｒｉｓｃｈｅｒ Ｅｌｅｋｔｒｏｔｅｃｈｎｉｓｃｈｅｒ Ｖｅｒｅｉｎ、Ｚｕｒｉｃｈ、Ｖｏｌ．８８、Ｎｏ．３，ｐｐ．２７－３０）。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Int. Sonal Application No
PCT/US 00/27685

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 420 866 A (WASILEWSKI ANTHONY J) 30 May 1995 (1995-05-30)	1,4,9
A	column 1, line 14 -column 7, line 7 figures 1-8	2,3,5-8, 10-16
P,X	WO 00 56068 A (THOMSON LICENSING S A ;DEISS MICHAEL SCOTT (US); ESKICIOGLU AHMET) 21 September 2000 (2000-09-21) page 2, line 14 - line 29 page 4, line 4 -page 5, line 14 figures 1-8	1,3
A	EP 0 858 184 A (NDS LTD) 12 August 1998 (1998-08-12) column 1, line 12 -column 7, line 20 figures 1-5	1-16

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 January 2001	06/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Tito Martins, J

4

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/27685

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" , EBU REVIEW-TECHNICAL,BE,EUROPEAN BROADCASTING UNION. BRUSSELS, NR. 266, PAGE(S) 64-77 XP000559450 ISSN: 0251-0936 the whole document	1-16
A	KRAMER D: "WUNDERKISTE DES DIGITALEN FERNSEHENS" , BULLETIN SEV/VSE,CH,SCHWEIZERISCHER ELEKTROTECHNISCHER VEREIN, ZURICH, VOL. 88, NR. 3, PAGE(S) 27-30 XP000886105 ISSN: 0036-1321 page 27-28	1-16

4

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/27685

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5420866 A	30-05-1995	AU 687844 B	05-03-1998
		AU 7220994 A	17-10-1995
		CA 2186368 A,C	05-10-1995
		JP 2940639 B	25-08-1999
		JP 9511369 T	11-11-1997
		WO 9526597 A	05-10-1995
WO 0056068 A	21-09-2000	AU 3629100 A	04-10-2000
EP 0858184 A	12-08-1998	IL 120174 A	28-10-1999
		GB 2322030 A,B	12-08-1998

Form PCT/ISA/210 (patent family annex) (July 1998)

フロントページの続き

(81)指定国 ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＭＺ，ＳＤ，ＳＬ，ＳＺ，ＴＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＧ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＢＺ，ＣＡ，ＣＨ，ＣＮ，ＣＲ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＤＭ，ＤＺ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＡ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＴＺ，ＵＡ，ＵＧ，ＵＳ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ

(72)発明者 マイケル スコット デイス
アメリカ合衆国 46077 インディアナ州 ジオンズビル インディアン パイプ レーン 1103
(72)発明者 ジャンールイ ディアスコーン
アメリカ合衆国 46032 インディアナ州 カーメル アーバー ドライブ 496
(72)発明者 デイビッド ジェイ ダフィールド
アメリカ合衆国 46220 インディアナ州 インディアナポリス フォール クリーク ロード 5459

Ｆターム(参考) 5C064 BA07 BB02 BC06 BC17 BC18 BC22 BC23 BD02 BD08 BD09 CA14 CB01 CC01 CC04
5J104 AA12 EA04 KA02 NA01 PA05